

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application)	
No. 09/973,301)	For: Method and Apparatus for
)	Security in a Data Processing
)	System
Hawkes et al.)	
)	
Examiner: David Garcia Cervetti)	
)	
Filed: October 9, 2001)	Group No. 2136

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

In response to the Notification dated 3/5/2007, Appellant submits the following remarks.

ELECTRONIC FILING

Transmitted electronically to the Patent and Trademark Office.

Depositor's Name: Tram O. Le
(type or print name)

Date: August 14, 2007

Signature: /Tram O. Le/

PATENT

The time period for response has been extended 5 months to 9/5/2007.

The Notification dated 3/5/2007 states that "The Appeal Brief filed 12/31/06 is non-compliant because it was unsigned." However, it is respectfully submitted that the Appeal Brief filed 12/31/06 was signed, see page 5 of the Appeal Brief. It appears that the Notification is referring to the last page of the attached appendix labeled "Copy Appeal Brief Appendix A" in which an un-signed copy was provided.

Therefore, Appellant submits another copy of the Appeal Brief filed on 12/31/06 with a signed last page of the attached appendix identified above.

Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: August 14, 2007

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. No. 40,457
(858) 651-6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

Appl. No. 09/973,301
Appellants' Brief

RECEIVED
CENTRAL FAX CENTER

DEC 31 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : Phillip Hawkes, et al.
Appl. No. : 09/973,301
Filed : 10/9/2001
Art Unit : 2136
Examiner : Cervetti, David Garcia
Title : Method and Apparatus for Security in a Data Processing System
Attorney Docket No. : 020002

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF

This is an appeal from the final Office Action dated November 29, 2005, rejecting claims 1-24.

(1) REAL PARTY IN INTEREST

The real party in interest is QUALCOMM Incorporated, the assignee of the entire interest.

(2) RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any related appeals, interferences or judicial proceedings.

(3) STATUS OF CLAIMS

The application was filed on October 9, 2001 with twenty-four (24) claims, of which Claims 1, 14, 18, and 21-23 are independent.

All of the claims were rejected in the non-final Office Action dated January 4, 2005.

In Appellants' response dated September 6, 2005, arguments were made indicating the patentability of Claims 1-24 over the proffered references.

The Examiner rejected all the claims in the final Office Action dated December 29, 2005.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of

Philip Hawkes et al.

For: METHOD AND APPARATUS FOR
SECURITY IN A DATA
PROCESSING SYSTEM

Serial No. 09/973,301

Filed: October 9, 2001

) Group No. 2136

Response to Notice of Non-Compliant AmendmentCommissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notice of Non-Compliant Amendment dated August 26, 2005, the amendment document filed on June 6, 2005 is hereby resubmitted with a complete listing of the claims.

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8(d))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

- ☐ deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Depositor's Name: _____
(type or print name)

Date: _____

FACSIMILE

- ☒ transmitted by facsimile to the Patent and Trademark Office on September 6, 2005.

Depositor's Name: Kate Lane
(type or print name)

Signature: _____

Dec 31 06 05:48p

Residence Inn By Marriott 319 395 0111

p.4

Appl. No. 09/973,301
Appellants' Brief

Appellants filed a Notice of Appeal dated May 30, 2006.

The status of the claims is as follows:

Claims rejected: Claims 1-24

Claims allowed: none

Claims withdrawn: none

Claims objected to: none

Claims canceled: none

Claims appealed: Claims 1-24

(4) STATUS OF AMENDMENTS

No amendment to the claims has been submitted since the final Office Action dated May 27, 2005.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1 provides:

A method for secure transmissions, the method comprising: determining a short term key for a message for transmission, the short term key having a short term key identifier; determining an access key for the message, the access key having an access key identifier; encrypting the message with the access key; forming an Internet protocol header comprising the short term key identifier; and transmitting the encrypted message with the Internet protocol header. (Specification, paragraphs 1066, 1072, 1078 and 1080; FIGS 4, 5A, 5B and 6, reference characters SK, SKI).

Independent Claim 14 provides:

A method for secure reception of a transmission, the method comprising: receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key; determining an access key based on the short term key identifier; encrypting the short term key identifier with the access key to recover the short term key; and decrypting the transmission using the short term key.

Appl. No. 09/973,301
Appellants' Brief

(Specification, paragraphs 1066, 1072, 1078 and 1080; FIGS 4, 5A, 5B and 6, reference characters SK, SKI).

Independent Claim 18 provides:

In a wireless communication system supporting a broadcast service option, an infrastructure element comprising: a receive circuitry; a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising: processing unit operative to decrypt key information; and a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message, comprising: memory storage unit for storing a plurality of short term keys and short term key identifiers.

(Specification, paragraphs 1066, 1072, 1078 and 1080; FIGS 4, 5A, 5B and 6, reference characters SK, SKI).

Independent Claim 21 provides:

An infrastructure element for a wireless communication system, comprising: means for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key; means for determining an access key based on the short term key identifier; means for encrypting the short term key identifier with the access key to recover the short term key; and means for decrypting the transmission using the short term key. (Specification, paragraphs 1066, 1072, 1078 and 1080; FIGS 4, 5A, 5B and 6, reference characters SK, SKI).

Independent Claim 22 provides:

A digital signal storage device, comprising: first set of instructions for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key; second set of instructions for determining an access key based on the short term key identifier; third set of instructions for encrypting the short term key identifier with the access key to recover the short term key; and fourth set of instructions for decrypting the transmission using the short term key. (Specification,

Appl. No. 09/973,301
Appellants' Brief

paragraphs 1066, 1072, 1078 and 1080; FIGS 4, 5A, 5B and 6, reference characters SK, SKI).

Independent Claim 23 provides:

A storage device having stored a communication signal transmitted on a carrier wave, wherein the communication signal comprising: a first portion corresponding to a short term key identifier, the short term key identifier having a corresponding short term key; and a second portion corresponding to a transmission payload encrypted using the short term key. (Specification; paragraphs 1066, 1072, 1078 and 1080; FIGS 4, 5A, 5B and 6, reference characters SK, SKI).

(6) GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Claims 21-24 stand rejected under 35 USC § 101 as allegedly being directed to non-statutory subject matter.

Claims 1-6 and 14-24 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Peirce et al. ("Pierce", U.S. Patent Number 5,467,398).

Claims 7-13 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Pierce in view of Nessett et al. ("Nessett", U.S. Patent Number 6,055,236).

(7) ARGUMENT

II. 35 U.S.C. § 102(b) Rejections

Claims 1-6 and 14-24

The issue is whether the Examiner has properly rejected Claims 1-6 and 14-24 under 35 U.S.C. § 102(b) as allegedly being anticipated by Pierce.

The applicant relies on the arguments made in the response mailed September 6, 2005, a copy of which is attached as Appendix A

Appl. No. 09/973,301
Appellants' Brief

III. 35 U.S.C. § 103(a) Rejections

A. Claims 7-13

The issue is whether the Examiner has properly rejected Claims 7-13 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Pierce in view of Nessett.

The applicant relies on the arguments made in the response mailed on September 6, 2005, a copy of which is attached as Appendix A.

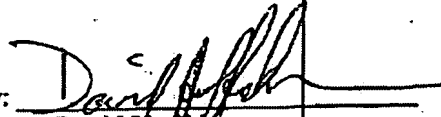
III. Conclusion

For the foregoing reasons, it is respectfully submitted that in each of the rejections discussed herein under 35 U.S.C. § 101, 102(b) and 103(a), the Examiner has failed to show that the proffered references teach or suggest each and every element of the claimed invention. Accordingly, reversal of all outstanding rejections is earnestly solicited.

Respectfully submitted,

Dated:

By:


David Huffaker
Reg. No. 56,771

Dec 31 06 05:49p

Residence Inn By Marriott 319 395 0111

P.8

Appl. No. 09/973,301
Appellants' Brief

(8) CLAIMS APPENDIX

Please see attached Appendix A

Appl. No. 09/973,301
Appellants' Brief

(9) EVIDENCE APPENDIX

None

(10) RELATED PROCEEDINGS APPENDIX

None

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

IN THE CLAIMS

Please amend the claims as follows:

1. (Original) A method for secure transmissions, the method comprising:
determining a short term key for a message for transmission; the short term key having a short term key identifier;
determining an access key for the message, the access key having an access key identifier;
encrypting the message with the access key;
forming an Internet protocol header comprising the short term key identifier; and
transmitting the encrypted message with the Internet protocol header.
2. (Original) The method as in claim 1, wherein the short term key identifier comprises the access key identifier.
3. (Original) The method as in claim 2, wherein short term key identifier further comprises a security parameter index value.
4. (Original) The method as in claim 3, wherein the security parameter index value is a random number.
5. (Original) The method as in claim 1, wherein the short term key is calculated as a function of the short term key identifier and the access key.
6. (Currently Amended) The method as in claim 5, wherein the short term key identifier is calculated by encrypting the short term key identifier with the access key.
7. (Original) The method as in claim 1, wherein the Internet protocol header is part of an ESP header.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

8. (Original) The method as in claim 7, wherein the Internet protocol header further comprises a second random number, the second random number having a random number identifier.
9. (Original) The method as in claim 8, wherein the short term key identifier comprises the access key identifier and the random number identifier.
10. (Original) The method as in claim 9, wherein short term key identifier further comprises a security parameter index value.
11. (Original) The method as in claim 10, wherein the security parameter index value is a random number.
12. (Original) The method as in claim 8, wherein the short term key is calculated as a function of the short term key identifier, the second random number, and the access key.
13. (Original) The method as in claim 12, wherein the short term key identifier is calculated by encrypting the short term key identifier and the second random number with the access key.
14. (Original) A method for secure reception of a transmission, the method comprising:
 - receiving a short term key identifier specific to a transmission; the short term key identifier corresponding to a short term key;
 - determining an access key based on the short term key identifier;
 - encrypting the short term key identifier with the access key to recover the short term key; and
 - decrypting the transmission using the short term key.
15. (Original) The method as in claim 14, further comprising:
 - storing the short term key identifier and short term key in a memory storage unit.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

16. (Original) The method as in claim 14, wherein the short term key identifier is comprised of a random number and an access key identifier associated with the access key.

17. (Original) The method as in claim 14, wherein encrypting the short term key identifier further comprises encrypting the short term key identifier and a random number with the access key to recover the short term key.

18. (Original) In a wireless communication system supporting a broadcast service option, an infrastructure element comprising:

a receive circuitry;

a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising:

processing unit operative to decrypt key information; and

a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message, comprising:

memory storage unit for storing a plurality of short term keys and short term key identifiers.

19. (Original) The infrastructure element as in claim 15, wherein the user identification unit further comprises a second memory storage unit for storing a plurality of access keys and access key identifiers.

20. (Original) The infrastructure element as in claim 15, wherein the memory storage unit is a secure memory storage unit.

21. (Original) An infrastructure element for a wireless communication system, comprising:

means for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key;

means for determining an access key based on the short term key identifier;

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

means for encrypting the short term key identifier with the access key to
recover the short term key; and
means for decrypting the transmission using the short term key.

22. (Original) A digital signal storage device, comprising:
first set of instructions for receiving a short term key identifier specific to a
transmission, the short term key identifier corresponding to a short term key;
second set of instructions for determining an access key based on the short
term key identifier;
third set of instructions for encrypting the short term key identifier with
the access key to recover the short term key; and
fourth set of instructions for decrypting the transmission using the short
term key.

23. (Currently Amended) A storage device having stored a communication signal
transmitted on a carrier wave, wherein the communication signal comprising:
a first portion corresponding to a short term key identifier, the short term
key identifier having a corresponding short term key; and
a second portion corresponding to a transmission payload encrypted using
the short term key.

24. (Original) The communication signal as in claim 23, wherein the short term
key identifier comprises:
a random number portion; and
an access key identifier corresponding to an access key.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

IN THE DRAWINGS

Enclosed herewith are amended Figures 1D in which the proposed changes are made in an annotated marked-up drawing with a replacement sheet.

IN THE SPECIFICATION

Paragraph 1051

Terminals 106A, 106B, 106C, 106D, 106E, 106F, 106G, 106H and 106I in the coverage area may be fixed (i.e., stationary) or mobile. As shown in FIG. 2, various terminals 106 are dispersed throughout the system. Each terminal 106 communicates with at least one and possibly more base stations 104 on the downlink and uplink at any given moment depending on, for example, whether soft handoff is employed or whether the terminal is designed and operated to (concurrently or sequentially) receive multiple transmissions from multiple base stations. Soft handoff in CDMA communications systems is well known in the art and is described in detail in U.S. Patent No. 5,101,501, entitled "Method and system for providing a Soft Handoff in a CDMA Cellular Telephone System", which is assigned to the assignee of the present invention.

Paragraph 1086

FIGS. 5A and 5B illustrate ~~FIG. 5B illustrates~~ the transmission and processing of keys, including RK, BAK and SK, according to an exemplary embodiment. As illustrated, at registration, the MS 300 receives the RK Information (RKI) and passes it to UIM 308, wherein the SUPU 316 computes RK using RKI and the A-key, and stores the RK in UIM memory storage SUMU 314. The MS 300 periodically receives the BAK Information (BAKI) that contains BAK encrypted using the RK value specific to UIM 308. The encrypted BAKI is decrypted by SUPU 316 to recover the BAK, which is stored in UIM memory storage SUMU 314. The MS 300 further periodically obtains SKI. In some exemplary embodiments, the MS 300 receives an SKI_RANDOM that it combines with SKI_PREDICT to form SKI. The SUPU 316 computes SK from SKI and BAK. The SK is provided to ME 306 for decrypting broadcast content.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

Paragraph 1098

FIG. 8B illustrates the subscription process in the system 500. The CS 502 further includes multiple encoders 504. Each of the encoders 504 receives one of the unique RKs and the BAK value generated in the CS 502. The output of each encoder 504 is a BAKI encoded specifically for a subscriber. The BAKI is received at the UIM of each MS, such as UIM₁ 512. Each UIM includes a SUPU and a SUMU, such as SUPU₁ 514 and SUMU₁ 510 of UIM₁ 512, and SUPU_N 534 and SUMU_N 530 of UIM_N 532. The SUPU includes a decoder, such as decoder 516 or decoder 536 that recovers the BAK by application of the RK of the UIM. The process is repeated at each subscriber.

Paragraph 1099

FIG. 8D illustrates the processing of BC after registration and subscription. The CS 502 includes an encoder 560 that encodes the BC using the current SK to generate the EBC. The EBC is then transmitted to the subscribers. Each MS includes an encoder, such as encoder 544 or encoder 554, that extracts the BC from the EBC using the SK.

Paragraph 1118

FIG. 13 illustrates operation 900 of the CS. For each IP packet, the transmitter determines the BAK that will be used to derive SK, and determines the BAK_ID corresponding to the BAK at step 902. The BAK_ID may be any type of identifier that allows discrimination among multiple BAK values. The CS sends BAK and the BAK_ID to individual users by performing subscription at step 904. The users may perform subscription at various times before and during the subscription period. Steps 902 and 904 may occur before the subscription period starts. At step 906 the transmitter selects a RAND value and determines the corresponding RAND_ID. At step 908, the CS may send RAND and RAND_ID to the MS individually or send RAND and RAND_ID to be broadcast on the broadcast channel. The value of RAND does not need to be secret, so it is not encrypted. If RAND and RAND_ID are broadcast, then there should not be much time between re-transmission so that an MS does not need to wait long before obtaining

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

the RAND value. Broadcasting RAND and RAND_ID will use a large amount of bandwidth over time. However, if there are a large number of users tuned to the channel, then a large amount of bandwidth will be required to send RAND to each user individually. Consequently, RAND and RAND_ID should only be broadcast if there are a large number of users tuned to the channel. At step 910 the CS chooses a random value of SPI RAND.

Paragraph 1119

Once the SPI RAND, BAK_ID and RAND_ID are known, the transmitter combines them (e.g., concatenates RAND_ID and BAK_ID to the SPI RAND) to form the SPI_SK at step 912. The CS uses a cryptographic function to combine SPI RAND, BAK (identified by BAK_ID) and RAND (identified by RAND_ID) to form SK at 914. The CS then encrypts the broadcast message or portion of the message with SK at step 916, and transmits the encrypted message at step 918. Note that the encrypted broadcast message is part of an IP packet that includes the IP header and the ESP header. The ESP header includes the SPI_SK. At decision diamond 920, the CS decides whether to change SK. If the CS decides not to change SK, then the CS proceeds to step 916. If the CS decides to change SK, then the CS proceeds to decision diamond 922, where the CS decides whether to change RAND. If the CS decides not to change RAND, then the CS proceeds to step 910. If the CS decides to change RAND, then the CS proceeds to decision diamond 924, where the CS decides whether to change BAK. If the CS decides not to change BAK, then the CS proceeds to step 906. If the CS decides to change BAK, then the CS returns to step 902.

Paragraph 1126

Continuing with FIG. 7C, the method 440 initializes the timer t2 at step 442 to start the SK_REG time period T2. The CS generates SK RAND and provides the value to transmit circuitry for transmission throughout the system at step 444. The timer t3 is initialized at step 446 to start the SK time period T3. The CS generates SK from SK RAND, BAK, and TIME at step 448. The CS then encrypts the BC using the current SK at step 450 448. The encrypted product is the EBC, wherein the CS provides the EBC to transmit circuitry for transmission in the system. If

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

the timer t2 has expired at decision diamond 452 450, processing returns to step 442. While t2 is less than T2, if the timer t3 has expired at decision diamond 454 452, processing returns to step 446, else processing returns to 450.

After paragraph 1127 and before paragraph 1128, insert the following:

FIG. 7E is a timing diagram of key update periods of a security option in a wireless communication system supporting broadcast transmissions.

Paragraph 1128

Key management and updates are illustrated in FIG. 8C, wherein the CS applies a function 508 to generate a value of SK_RANDOM, which is an interim value used by the CS and MS to calculate SK. Specifically, the function 508 applies the BAK value, the SK_RANDOM and a time factor. While the embodiment illustrated in FIG. 8C applies a timer to determine when to update the SK, alternate embodiments may use alternate measures to provide periodic updates, for example occurrence of an error or other event. The CS provides the SK_RANDOM value to each of the subscribers, wherein a function 518 or 538 resident in each UIM applies the same function as in function 508 of the CS. The function 518 operates on the SK_RANDOM, BAK and a timer value to generate a SK that is stored in a memory location in the ME, such as MEM₁ 542 of ME₁ 540 and MEM_N 552 of ME_N 550.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

REMARKS

Claims 1-24 are pending in the present application, of which claims 1, 14, 18 and 21-23 are independent. Claims 6 and 23 have been amended. After entry of the above amendments, claims 1-24 are pending in the present application, of which claims 1, 14, 18 and 21-23 are independent.

Applicants believe that the present application is in condition for allowance, which prompt and favorable action is respectfully requested.

I. DRAWINGS

Enclosed here herewith is amended Figure 1D in which the proposed changes are made. Applicant respectfully requests the Examiner to accept these Figures as amended because they correct informalities pointed out by the Examiner.

With respect to Figures 2, 5A, 7C, 7E, 8B-D and 13, Applicants have amended the corresponding specification to add the reference character(s) pointed out by the Examiner. Applicants submit that the amendments have been made to correct the informalities and not to narrow the scope of the claim. Also, the amendments are disclosed in the respective Figures such that no new matter has been submitted.

Therefore, Applicants respectfully request withdraw of the objection to the drawings.

II. CLAIM OBJECTIONS

Applicants would first like to thank the Examiner for the careful review and for pointing out the informalities in claim 6. Claim 6 has been amended to correct the informality and not to narrow the scope of the claim.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

With respect to claim 7, Applicants submit that the term "ESP" has been defined in paragraph 1068. If the Examiner wishes, Applicant can amend the claim to spell out the Acronym.

III. CLAIM REJECTION UNDER 35 U.S.C. §101

The Examiner rejected claims 21-24 as having non-statutory subject matter. Applicants respectfully disagree.

With respect to claim 21, Applicants submit that the subject matter has expressed an apparatus by the means for performing a specified function as defined in 35 U.S.C. §112 sixth paragraph. Therefore, claim 21 is permitted and not non-statutory.

With respect to claim 22, Applicants submit that the subject matter claimed is "a digital signal storage device" and not just the digital signal. Also, Applicants submit that software is considered statutory subject matter if there is a medium involved. Since the subject matter of claim 22 involves a storage device, claim 22 is not non-statutory.

With respect to claims 23 and 24, Applicants have amended claim 23 and believe that the subject matters are also not non-statutory.

Accordingly, Applicants respectfully request withdrawal of the rejection under 35 U.S.C. §101.

VI. REJECTION UNDER 35 U.S.C. §102

The Examiner rejected claims 1-6 and 14-24 under 35 U.S.C. §102(b) as being allegedly anticipated by U.S. Patent No. 5,467,398 issued to Pierce et al. (hereinafter "Pierce"). The rejection is respectfully traversed in its entirety.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

To anticipate a claim under 35 U.S.C. §102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

Pierce discusses a typical key exchange between a subscriber unit and an infrastructure communications center. In the section cited by the Examiner, it teaches providing a messaging key and associated subscriber unit reference number to the subscriber unit and the infrastructure communications center. Pierce also teaches generating an authentication key and identifier at either the subscriber unit or the infrastructure communications center. The authentication key with the identifier is then encrypted using the messaging key and communicated to the entity that did not generate the key (col. 2, lines 42-58). Thereafter, authentication key is used periodically by the infrastructure communications center to verify the subscriber unit (col. 4, lines 30-35).

Pierce does not teach or even mention a short term key as in independent claims 1, 14, 18 and 21-23. It does not teach or even suggest encrypting a message with an access key, forming an Internet protocol header comprising a short term key identifier or transmitting the encrypted message with the Internet protocol header as in claim 1. It does not teach or even suggest receiving a short term key identifier specific to a transmission, encrypting the short term key identifier with the access key to recover the short term key or decrypting the transmission using the short term key as in claims 14 and 21-22.

Accordingly, since Pierce does not teach every element of the claims, Applicants submit that Pierce does not anticipate claims 1, 14, 18 and 21-23. Also, claims 2-6, 15-17, 19-20 and 24 depend from and include all the elements cited in the independent claims 1, 14, 18 and 21-23, respectively. Accordingly, Applicant submits that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

COPY APPEAL BRIEF APPENDIX A

Attorney Docket No. 020002

Therefore, Applicants respectfully request a withdrawal of the rejection under 35 U.S.C.

§102 for at least the foregoing reasons.

V. REJECTION UNDER 35 U.S.C. §103

The Examiner rejected claims 7-13 under 35 U.S.C. §103 as being unpatentable over Pierce in view of U.S. Patent No. 6,055,236 issued to Nessett et al. (hereinafter "Nessett").

To establish a prima facie case of obviousness for a claimed invention, all the claim elements must be taught or suggested by the prior art. (MPEP 2143.03)

Claims 7-13 depend from and include all the elements cited in the independent claim 1. Accordingly, Applicant submits that Pierce does not disclose every element of claims 7-13 based on its dependency from claim 1 as well as other novel features included therein. Nessett also does not teach a short key or Internet protocol header as in independent claim 1.

Since neither Pierce nor Nessett, separately or combined, teach or suggest all the elements, Applicants respectfully submit that the Examiner has failed to set forth a prima facie case of obviousness and respectfully requests that the rejections of claims 7-13 be withdrawn.

CONCLUSION

In light of the response contained herein, Applicants submit that the application is now in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: September 6, 2005

By: _____

Jae Hee Choi, Reg. No. 45,288
(858)651-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502